Defense Horizons

Number 16

A publication of the
Center for Technology and National Security Policy
National Defense University

AUGUST 2002

# The Virtual Border: Countering Seaborne Container Terrorism

*by Hans Binnendijk, Leigh C. Caraher, Timothy Coffey, and H. Scott Wynfield*

## Overview

America's potential vulnerability to terrorist attack through exploitation of the global trade and transportation system is now widely recognized. The sheer magnitude and diversity of this global system coupled with the permeability of U.S. borders afford numerous avenues to attack American targets. Maritime commerce, and container shipping in particular, provides a highly attractive means not only of delivering weapons but also of smuggling terrorists themselves into the American homeland. Thousands of ships from every part of the globe deliver millions of individual containers to American ports each year. Compounding the problem is an inspection process that has been slow to shift from more traditional practices, such as the search for illegal narcotics, to the search for terrorist weapons. This situation stems in part from a lack of information specifying cargo contents, complicating U.S. Customs Service efforts to identify high-risk containers for inspection upon arrival, and from the commercially driven need to move trade goods rapidly through the transportation system. The problem does not end at the American shoreline, however. The intermodal transportation network, encompassing sea, land, and rail linkages, represents a vast conduit that could be exploited for an attack on not only port facilities and marine terminals but also inland population centers and shore infrastructure. By using global positioning system technology, terrorists may achieve precision targeting capabilities and create a "poor man's" intercontinental ballistic missile from a container.

Reducing the risk of terrorism from seaborne containers is not just a U.S. border management problem. Once the container arrives at a U.S. port, it may already be too late to prevent catastrophic consequences. Nor is maritime interdiction of suspicious cargo an optimal approach due to both the practical problem of sorting through thousands of stacked containers and the massive economic disincentives associated with diverting or inspecting cargo once loaded aboard ship. The primary objective must be to establish a high degree of confidence that containers earmarked for U.S. destinations are secure before they leave a foreign port. The first and most important line of defense against container terrorism, therefore, is at the foreign point of origin. U.S. control over cargo bound for American shores should begin there, creating, in effect, a *virtual border.* This virtual border must be designed to provide a multilayered defense, addressing container security from the initial loading of the container to its movement through the entire international transportation network.

Implementation of a virtual border security program, however, must maintain the economic viability of seaborne commerce. Security planners must determine how best to construct a security system that substantially reduces the threat from container terrorism yet still guarantees an uninterrupted flow of trade goods. Likewise, the right balance must be struck between implementation cost and mitigation of risk. This is a multifaceted problem involving a mix of security, economic, technological, and foreign policy considerations, and any solution will require a comprehensive, integrated, and international approach.

**Center for Technology and National Security Policy**

The National Defense University (NDU) established the Center for Technology and National Security Policy in June 2001 to study the implications of technological innovation for U.S. national security policy and military planning. The center combines scientific and technical assessments with analyses of current strategic and defense policy issues. Its major initial areas of focus include: (1) technologies and concepts that encourage and/or enable the transformation of the Armed Forces, (2) developments by defense laboratories, (3) investments in research, development, and acquisition and improvements to their processes, (4) relationships among the Department of Defense, the industrial sector, and academe, and (5) social science techniques that enhance the detection and prevention of conflict. The staff is led by two senior analysts who hold the Roosevelt Chair of National Security Policy and the Edison Chair of Science and Technology and who can call on the expertise of the NDU community and colleagues at institutions nationwide. The papers published in the *Defense Horizons* series present key research and analysis conducted by the center and its associate members.

# Report Documentation Page

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE | 2. REPORT TYPE | 3. DATES COVERED |
|---|---|---|
| **AUG 2002** | **N/A** | **-** |

| 4. TITLE AND SUBTITLE | 5a. CONTRACT NUMBER |
|---|---|
| **The Virtual Border: Countering Seaborne Container Terrorism** | 5b. GRANT NUMBER |
| | 5c. PROGRAM ELEMENT NUMBER |
| 6. AUTHOR(S) | 5d. PROJECT NUMBER |
| | 5e. TASK NUMBER |
| | 5f. WORK UNIT NUMBER |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Defense University Center for Technology and National Security Policy Fort McNair Washington, DC 20319** | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR'S ACRONYM(S) |
| | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) |

12. DISTRIBUTION/AVAILABILITY STATEMENT
**Approved for public release, distribution unlimited**

13. SUPPLEMENTARY NOTES
**The original document contains color images.**

14. ABSTRACT

15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT **unclassified** | b. ABSTRACT **unclassified** | c. THIS PAGE **unclassified** | **UU** | **12** | |

Establishment of a virtual border security program requires improvements in three key areas of container shipping: cargo certification, physical security, and inspection. Procedures such as use of trusted foreign shippers will establish a higher degree of confidence that only legitimate cargos are loaded for container shipping, and utilization of better container seals coupled with improved security at port and container storage facilities will help prevent terrorists from gaining easy access to cargo and containers. More sophisticated container inspection techniques will require timely and accurate information on individual container shipments and the introduction of container profiling based on comprehensive data collection and analysis. Receiving detailed data before a cargo is shipped and analyzing this data by fusing it with data from other commercial and intelligence sources will enable rapid identification of suspicious shipments. In addition, better detection technology is needed to complement the inspection process.

**a terrorist attack anywhere within the international trading system would have an adverse effect upon the system worldwide**

All of these improvements will require a high level of both domestic and international cooperation. On the domestic front, the U.S. Government, working in concert with the business community, needs to develop a comprehensive national strategy. Key components of this strategy must include the delineation of clear lines of interagency authority and responsibility and the identification of additional legislative changes that might be necessary to bolster the security of commercial practices in economically sound ways. On the international front, exporting states need to assume greater responsibility for container shipping security. Diplomatic initiatives will be required to establish agreements on intelligence sharing, container security standards, and global shipping practices. Despite the numerous vulnerabilities associated with container shipping and the seeming intractability of the problem, an international program based on the concept of the virtual border can substantially reduce the risk from seaborne container terrorism.

## Background

In October 2001, the Center for Technology and National Security Policy (CTNSP) initiated an independent, unclassified study to address the potential terrorist threat posed by seaborne container shipping. Participants included a multidisciplinary team of specialists drawn from the technology, policy, and transportation communities within the National Defense University and other government and private organizations.[1] The purpose of the study was to analyze the characteristics of the container threat and suggest ways in which the security of seaborne container shipping might be improved, particularly through the use of detector technologies. The study focused on the seaborne importation of containers into the United States, although it was recognized that U.S.-exported containers and containers entering the country through air and land routes present similar threats. Participants also acknowledged that container security is truly an international problem and that a terrorist attack anywhere within the international trading system would have an adverse effect upon the system worldwide.

To inform the policy debate, the findings of the study were presented earlier this year as a series of briefings to personnel representing agencies involved in various aspects of maritime and transportation security. This article summarizes the findings of the study and subsequent CTNSP research.

## The Seaborne Container Threat

The a priori assumption of America's vulnerability to terrorist attack via seaborne container shipping was based on the nature of the global container shipping industry. The numbers of containers entering the United States, the manner in which these containers move through the international transportation system, and the weaknesses in container documentation and inspection processes all contribute to the attraction of containers as terrorist weapons. World Shipping Council estimates underscore the magnitude of the potential problem: approximately 800 oceangoing liners and their multinational crews make more than 22,000 port calls in the United States each year. Consisting primarily of container ships and roll-on/roll-off vessels, these liners from every part of the globe deliver to the United States approximately 7.8 million containers of imported cargo per year—an average of 20,000 containers per day—and these numbers are growing dramatically.[2] At the Los Angeles-Long Beach port complex, for example, one of the Nation's largest and busiest port facilities, officials estimate that port traffic will double over the next 2 decades. The planned mile-long wharfs will accommodate up to six new generation cargo vessels with the capacity to carry as many as 15,000 containers. Dozens of computerized cranes will offload these containers onto endless lines of waiting 18-wheelers and hundreds of trains.[3]

The container industry is a remarkably efficient commercial system, designed to move goods through the international marketplace in the most expeditious manner, but it is not an industry designed for security. Speed and cost are the overriding drivers in this system. There are no economic incentives either to perform cargo inspections or to generate paperwork beyond what is essential to move containers through the various stages of shipping. The huge volume of container traffic and the usually lax controls over cargo packing and shipping provide ample opportunities to introduce a

**Hans Binnendijk holds the Roosevelt Chair of National Security Studies and is the Director of the Center for Technology and National Security Policy (CTNSP) at the National Defense University. Dr. Binnendijk may be contacted at (202) 685–2557 or via e-mail at binnendijkh@ndu. Leigh C. Caraher is a research analyst at CTNSP, and may be contacted at (202) 685–2659 or via e-mail at caraherl@ndu.edu. Timothy Coffey holds the Edison Chair of Science and Technology at CTNSP, and is a senior research scientist at the University of Maryland. Dr. Coffey may be reached at (202) 685–2658 or via e-mail at coffeyt@ndu.edu. H. Scott Wynfield is a research fellow at CTNSP, where he may be contacted at (202) 685–2530 or via e-mail at wynfieldh@ndu.edu.**

weapon into a container at several stages in the transportation process. The increasing magnitude and speed of this trade is already sufficient to overwhelm existing inspection processes. Unless changes are introduced, a weapon probably could arrive at a U.S. port undetected.

While an attack on an American port would yield serious consequences, the threat is not restricted to ports alone; inland sites are equally at risk. From the port of entry, containers enter a vast transportation network of truck, rail, and inland waterway routes over which they are delivered to American addresses or carried in bond en route to international destinations. Several thousand containers move along major transportation arteries throughout the U.S. mainland daily, exposing numerous urban centers and facilities such as nuclear power plants, chemical and oil refineries, hazardous material storage sites, and key transportation infrastructure to attack. Along the Houston Ship Channel, for example, there are 150 such sites that might be vulnerable.[4]

Using simple mechanical triggering devices or more sophisticated technology based on the global positioning system (GPS), for instance, a weapon-carrying container may be readily transformed into a precision-guided munition. Using such technology, several containers, perhaps arriving on opposite coasts, might be configured to attack selected targets in different parts of the country with near simultaneity. An attack on this scale has the potential to cause devastating loss of life in addition to perhaps billions of dollars in damage to the U.S. economy. Furthermore, the massive economic disruption that would be created by such an event, particularly in this era of increasing global reliance on seaborne commerce, might effectively shut down global trade for a prolonged period of time.

To assess the threat from a terrorist attack utilizing a container imported into the United States, the study team posited several operational scenarios. The objective of this approach was to characterize the most immediate risks to suggest appropriate near-term countermeasures, particularly the use of detector technologies. Two operational scenarios were considered probable. First, the weapon could be placed in the container at an overseas loading point, and terrorists could mask the contents by making the shipment appear to be legitimate. Second, the weapon could be introduced surreptitiously into a legitimate container shipment somewhere along the transportation route. In both cases, the weapon might be designed either to detonate at a specific point along the route or to be retrieved by an agent for subsequent use. The study team recognized that weapons could be obtained or assembled domestically and placed in a shipping container for export. This scenario was not examined in detail because the study focused on the threat of imported containers.

The characteristics of a specific container threat are based on the type of weapon that might be employed, the probability that terrorists would have access to their weapon of choice, and the likelihood of using a seaborne container as the means of delivery. The container itself seems ideally suited for mounting a terrorist attack. The abundant cargo space of the international standard 8-foot-by-8-foot container, which ranges in length from 20 to 48 feet, affords a convenient vehicle to convey both large devices, in which the container itself may be part of the weapon, and small, concealed devices, intended for receipt and use by an agent in country.[5] Thus, nuclear, radiological, and large conventional explosive devices could be employed as well as chemical, biological, or smaller conventional devices. The arrest by Italian police of an Egyptian man in a well-provisioned container in October 2001 demonstrates that containers might also be used to transport terrorists themselves.

From the range of possibilities, the study team concluded that containers carrying a radiological bomb or Stinger-like antiaircraft missile represent the most significant near-term threats. In both cases, a seaborne container was judged an ideal mode of transportation, while utilization of either device had the potential to cause large-scale loss of life and create substantial economic disruption. In the case of a radiological weapon, it was deemed probable that the radioactive material and chemical explosives needed to construct a "dirty bomb" could be obtained from foreign sources, and the device could be shipped by container from a different country.[6] Similarly, the relatively small Stinger missile could easily be smuggled in a container. The Taliban are believed to have an unknown number of American-supplied Stinger missiles left over from the war against the Soviet Union, and they may have obtained more from other international sources.

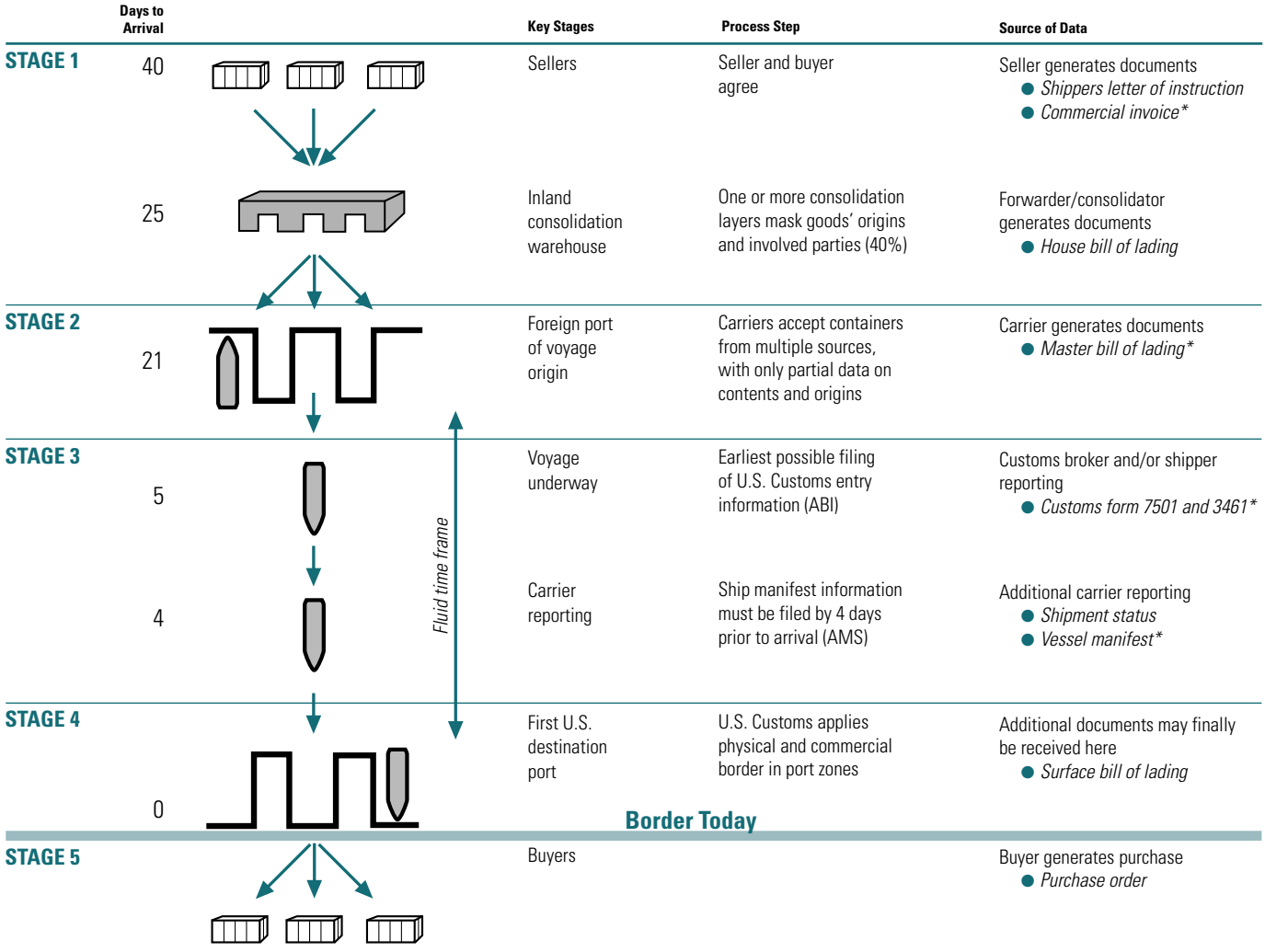
**containers carrying a radiological bomb or Stinger-like antiaircraft missile represent the most significant near-term threats**

Although this assessment highlights radiological devices and Stinger-like missiles as probable weapons, other weapons may also be employed in a seaborne container (though this is relatively less probable in the near term). A nuclear weapon would certainly produce the greatest destruction, but terrorist possession of such a weapon was deemed less probable at the time of the study. Also, if one were acquired, it might prove too valuable an asset to relinquish control over it by shipping in a container. In the case of biological weapons, the smaller size of the weapon containers makes such devices readily transportable by means other than a container. Since containers are routinely used to ship chemicals, the study team believed conventional explosives might be utilized in conjunction with legitimate chemical shipments to magnify the destructive effect of the explosion. Stand-alone conventional explosives, similar to the fertilizer bomb used in Oklahoma City, could also be employed, but because a weapon of this type could be assembled domestically, an imported container may be a less likely source of transport. While these conclusions represent the team's assessment of the relative threat at the time of this study, the threat is likely to evolve significantly as particular weapons become more available and as terrorists adapt to new security measures designed to prevent the use of containers as transport vehicles.

## The Container Domain

When an American buyer creates a typical purchase order for goods from a foreign seller, an elaborate process involving multiple parties is set in motion. In addition to the original importer and

**Figure 1. The Container Domain**




*Documents reported to U.S. Customs Service

exporter, financial and insurance institutions, inland transporters, freight consolidators, dockworkers, ocean carriers, and several government agencies are involved. A typical trade may generate 30 to 40 documents with scores of data elements, many of which involve a manual exchange of information. In the United States alone, these transactions involve numerous commercial entities: approximately 400,000 importing and exporting companies, 4,000 licensed forwarders and customs brokers, several thousand consolidators, and countless freight haulers. On a global basis, several million individuals are engaged in some stage of the container transportation industry.[7] The full scope of this shipping process must be addressed to build an effective response to the container threat. Figure 1 illustrates five key stages in the container transportation domain, each having unique characteristics that must be addressed in constructing a comprehensive security plan.[8]

From a counterterrorism perspective, the most critical stage in this process involves the initial transactions between buyer and seller, including generation of the initial shipping documents, loading and sealing of the container, and its delivery to the exporting port. In current commercial practice, individuals or companies may order, load, and seal a container, providing only scant detail on the contents and ownership of the cargo. In some instances, container cargo is shipped through inland consolidators, where a number of smaller orders may be combined to produce a full container load. In this transit phase, suppliers, packers, freight consolidators, and transporters will handle the cargo and container box. Such business practices make it more difficult to know precisely the contents of a particular container and the true identity of the original shipper.

Once a container is sealed and enters the transportation system, the security problem is further exacerbated because the container is not secured as it moves through the system. As a result, the

integrity of the container box is subject to compromise, particularly after it arrives at a foreign port for the second stage of its journey. Here a number of factors contribute to the problem. The absence of stringent sealing requirements for container boxes, lax physical security, and minimal inspection at some foreign ports, coupled with limited U.S. oversight at these ports, all create security risks. A similar problem exists once the vessel is under way and the ship's crew and passengers and workers at port stops come into contact with the containers along the ship's route of transit. The fact that U.S. Customs Service inspectors routinely find broken seals on containers, most likely opened to pilfer the contents, indicates vulnerability to tampering after initial loading.

Since the current Customs system was designed primarily for economic protection, shipping documentation requirements are structured to provide information related to commerce. With the exception of hazardous material, exporters may not report to the carrier the exact contents of the cargo, and the information that shippers provide is often intentionally misleading, designed to protect forwarders from competition by carriers, to avoid tariffs, or to protect the cargo from theft.[9] Even when there is no attempt to obfuscate, the cargo shipping information is often neither accurate and complete nor timely enough to allow for effective screening to identify potential terrorist threats. As figure 1 illustrates, much of the data is reported after the ship is under way or even after its arrival in the United States. Documents such as the commercial invoice and master bill of lading normally provided to U.S. Customs inspectors consist of only that information necessary to ensure compliance with Customs rules and tariff requirements.

**the U.S. Government needs substantially better visibility into the entire container domain, particularly the first stage in the shipping process**

Once a shipment arrives at a U.S. port, Customs inspectors are faced with the problem of determining which containers among the thousands to inspect. Under current procedures, approximately 2 percent of containers are selected for inspection to ensure compliance with U.S. laws governing importations, to determine appropriate entry of restricted merchandise such as hazardous material, and to intercept prohibited items such as narcotics and other contraband. Transiting the country en route to other foreign destinations, containers shipped under a customs bond are often subject to even less scrutiny.[10] While counterterrorism is now a priority within U.S. Customs, adequate procedures for inspection have not yet been implemented.

Although the current percentage of containers inspected upon entering the country may appear small, determining if this figure represents the "right" containers is more important than the actual number of containers inspected. To make this determination, the U.S. Government needs substantially better visibility into the entire container domain, particularly the first stage in the shipping process. It is important both to verify the specific contents of a cargo and to establish the identity of the shipper prior to container loading. If this verification does not take place, a more stringent mechanism for inspecting the container is required. Simply speaking, it is necessary to push the U.S. border back to create a virtual border in the country of origin to establish a high degree of confidence that container cargo bound for American shores is safe. Security initiatives, however, must not end at the port of embarkation. The concept of a virtual border implies not simply a fixed line at the foreign shoreline but rather a multilayered defense for the end-to-end movement of cargo throughout the container domain.

## Shoring Up the System

Creating an effective virtual border security program requires improvements in three essential areas: creating an initial certification process; enhancing the physical security of the standard shipping container; and creating a more sophisticated inspection system using container profiling and better detection technology.

A fundamental goal of the virtual border approach is to establish a certified cargo in which a container's contents are well documented, verified, and approved prior to shipping to the United States. Accomplishing this entails establishment of minimum data requirements and a tighter reporting timeline for commercial documentation. The sources of data shown in figure 1 might be combined with other commercial documents, such as financial data and inland transportation information, to provide a complete picture of the transaction, the parties involved, and the transportation plan. Prescreening of cargo will allow Customs to authorize shipment to the United States before loading rather than waiting until the shipment is under way, as in current practice. Creating a new electronic security questionnaire enabling rapid, automated screening and certification of container cargo would expedite this process and minimize costly delays. To facilitate the certification process, the Customs Service will need to station its officials at overseas ports.

Shippers complying with physical security requirements for containers and participating in this electronic inspection and certification process would be designated *trusted agents*. They might receive economic incentives through the use of "green lane" passes designed to expedite their shipments through the maritime system. Such rewards might be balanced by penalties. Shippers who are unable or unwilling to comply might find their shipments delayed until physical inspection of the contents can be completed. Rather than utilizing simple go or no-go criteria for cargo certification, a ranking system could be employed that would assign levels of risk for each container. Such a ranking system could also be useful in allocating limited inspection resources.

A second objective is to ensure that contents remain secure by enhancing the physical security of the container itself, which requires improvements in both the integrity of the container box and the environment in which it moves, particularly the port facility. Physical security must begin at loading with the use of international standard, registered, and tamper-resistant container seals,

and inclusion of seal numbers on all shipping documentation. The integrity and serial number of the seal could be checked as the container passes to different parties in the transportation process. Broken or missing seals would constitute cause to refuse acceptance. If the container must be opened for any reason, a new seal would need to be affixed and the new seal number recorded in the container documentation.

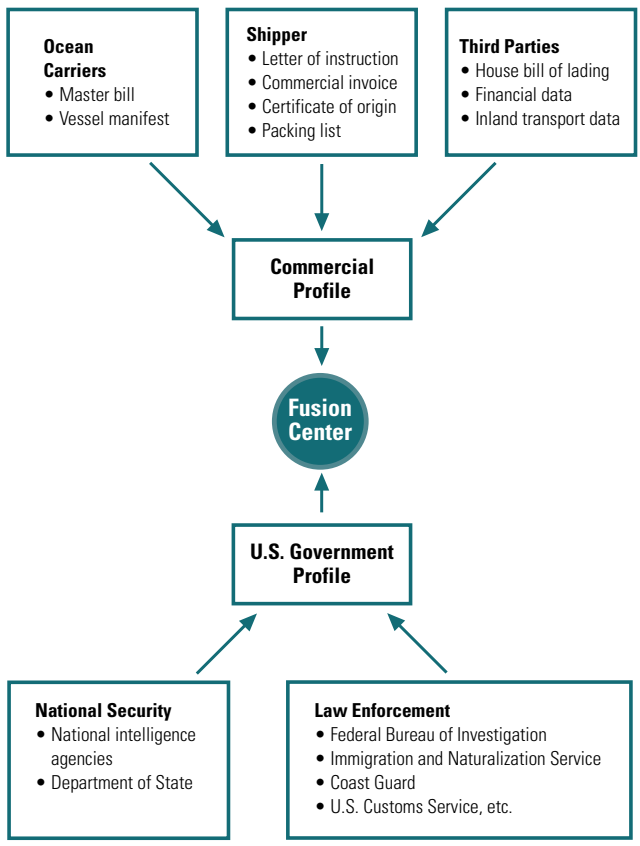
Proposals for electronic sealing, sensing devices inside a container to indicate tampering, and utilizing GPS-based technology to provide precise container location information have been suggested. While such devices would contribute to the physical security of the container box, the implementation of these devices in the near term might prove both impractical and prohibitively expensive, given the millions of containers in the international system. More research is therefore needed to determine the optimal future approach to economically ensuring container integrity.

As important as proper sealing is protecting the container from unauthorized access while in port or in a storage facility. To ensure that access is restricted to authorized personnel and vehicles, international minimum standards for marine terminal security should be established. These standards might include requirements to establish port security plans and to credential certain types of port workers. In areas where containers are stored temporarily, attention must be given to adequate fencing, lighting, and access control points. Sufficient numbers of trained security personnel also are needed to conduct routine monitoring and inspections of container shipments.

Improving the completeness and timeliness of container cargo information and protecting the container itself are only part of the solution. Creating a more sophisticated inspection process will require individual container profiling, a continuous process that begins with the initial certification of the cargo and continues until the container arrives at an American port. Profiling entails the collection and analysis of not only the commercial data supplied by shippers, ocean carriers, and third parties but also national security and law enforcement information. When this broad range of information is combined at a fusion center (shown notionally in figure 2), a more comprehensive security assessment of containers, ships, and crews can be created. Container profiling based on this national-level analysis will make it easier to identify with greater precision suspicious cargos that could be held at a foreign pier or interdicted under way.

The operation of the fusion center is inherently a government-wide responsibility dependent on all-source information and a high level of cooperation among numerous U.S. Government agencies. Many information and data collection systems that could provide input to the fusion center already exist or are under development within agencies responsible for various aspects of the container problem. For example, the Customs Automated Commercial Environment and the International Trade Data System (a multiagency effort) currently under development promise significant improvements in capturing the data necessary to profile containers.

**Figure 2. Fusion Center**




To ensure a systematic and integrated approach to the development of these and other data collection systems for container profiling, an interagency architecture is required. Among the first steps toward establishment of the fusion center must be a review of existing agency information systems, a determination of data requirements for container profiling, and the development of a plan to integrate these systems. Operational and technical architectures specifying standard data reporting formats and secure interagency communications links are needed before a real-time, accessible container database can be created.

**improving the completeness and timeliness of container cargo information and protecting the container itself are only part of the solution**

The development of new data analysis methodologies and advanced computational techniques will optimize the fusion center's product. This will require establishing rule sets to recognize the relationships between disparate pieces of information and to identify certain patterns or discrepancies. Risk assessment algorithms may then be created based on current understanding of the shipping industry to identify anomalies in the shipping process. Anomalies that could be targeted include document discrepancies, cargo incongruous with its origin, suspicious parties involved in the

transaction, suspect routing or shipping prioritization, and any other contradiction or violation of commercial shipping practices.

Analyzing all-source data in new ways may also provide wholly new insights into potential threats. When commercial data pertaining to an otherwise innocuous cargo, perhaps precertified as safe, is combined with vessel tracking information, crew lists, and a report of a probable terrorist presence in a port of call, red flag indicators would be triggered, even though any of these individual events would have been insufficient to produce a warning.

Even more sophisticated analysis may be achieved with advanced computational techniques in which the fusion center's meta-database is combined with anticipatory or predictive models and search strategies. By providing quantitative and qualitative insights into the complex behavior of terrorist organizations, agent-based modeling and simulation, or artificial neural networks, could generate new pattern recognition algorithms, which in turn would shape new search strategies and produce new risk assessment programs. In anticipation of evolving threats, in which terrorists seek to mask behavioral patterns that would identify their actions, evolutionary analysis may provide an effective means of discovering such patterns. These evolutionary, or genetic, algorithms would be used to develop offensive strategies potentially used by terrorists and to suggest defensive counterstrategies. The combination of a meta-database and anticipatory modeling would enable the fusion center to identify current container threats better and anticipate probable future threats as terrorists adapt to our defenses.

**the inspection process can be further enhanced by the use of sophisticated detection devices capable of identifying nuclear weapons, radiological materials, chemical and biological agents, and conventional explosives**

## The Role of Detectors

Improvements in the inspection process through container profiling can be further enhanced by the use of sophisticated detection devices capable of identifying nuclear weapons, radiological materials, chemical and biological agents, and conventional explosives. Employing these devices at ports of embarkation, where containers are loaded onto vessels, is an important element in creating a virtual border. If a terrorist container does enter an American seaport, these countermeasures would also provide the final line of defense. Therefore, this study undertook an initial survey of detector technologies. The survey was restricted to unclassified literature and focused on available detector technologies rather than providing a comprehensive assessment of their potential applications. The intent was to examine technologies suitable for use on closed containers in a port environment where speed, ease of use, and low false alarm rates are critical.

## Nuclear Material Detection

In the case of a nuclear weapon, the principal interest is in the detection of gamma radiation and/or neutrons emitted as a result of spontaneous fission or some stimulation process. In the case of radiological weapons, it is the detection of gamma radiation. (Table 1 provides a summary of several relevant technologies.) One of the best understood passive detectors for nuclear radiation is the sodium iodide crystal coupled with a photomultiplier tube. The detection range for weapons-grade quantities of fissile materials,

**Table 1. Nuclear Detection**

| Type | Technology | Size | Characteristics |
|---|---|---|---|
| Passive gamma ray | Sodium iodide crystals and photomultiplier tube | 3-inch crystals | Robust, high false alarm rate at high sensitivity, poor spectral resolution |
| Passive gamma ray | Germanium | 3-inch crystals | Sophisticated instrument, needs refrigeration, very high resolution (does not make mistakes) |
| Passive gamma ray | Mercuric iodide | Few square inches | Intermediate spectral resolution, solid-state, robust, relatively expensive |
| Passive neutron | Scintillating glass fibers | 100 square inches | Robust, solidstate, wound to desired geometry |
| Passive solidstate neutron | CMOS/SOI* | Small (like cell phones) | Relatively inexpensive, small, no real database on utility in real world |
| Geiger counters | Simple ionization chamber | Hand-held | Not specific, low sensitivity, relatively inexpensive |
| Active neutron interrogation | Pulsed neutron source | Large | Sophisticated instrument, radiation hazard |
| Active gamma ray scanner | Pulse power | Large | Robust technology, radiation hazard, good spatial resolution, imaging |

*Complementary metal oxide semiconductor/silicon on insulator

which is small on land due to the interference of natural background radiation, improves slightly over water. The relatively compact sodium iodide system tends to have a high false alarm rate when operated at high sensitivity and has poor spectral resolution of the gamma ray radiation being measured.

A second class of well-understood gamma radiation detectors is made from high-purity germanium crystals. These crystals are typically similar in size and detection ranges to the sodium iodide crystals. The high-purity germanium system has a very high spectral resolution for the gamma radiation being measured and generally does not make a mistake in identifying the device responsible for the gamma radiation. However, this system is quite sophisticated and requires refrigeration. Compact versions of these detectors are now being produced.

A relative newcomer in nuclear gamma radiation detection is the mercuric iodide detector. This detector has a spectral resolution between that of sodium iodide and high-purity germanium. It has the advantages of being an all-solid-state system and requiring no refrigeration. However, it is relatively expensive when produced in the size that would be needed for the port application.

The classic detector for neutrons produced as a result of spontaneous fission is the Helium-3 gas proportional counter. These devices are well understood and tend to be relatively bulky. The detection ranges for neutrons are similar to those for gamma radiation. In recent years, specially treated glass fibers have been produced and commercialized for the purpose of neutron detection. This technology has the distinct advantage of being able to be wound so as to produce specific geometric shapes that might be advantageous for neutron detection. A typical panel for a neutron detector built from these classes of fibers might be about 100 square inches in size. These devices also have the advantage of being all solid-state.

Unlike previously mentioned detectors, complementary metal oxide semiconductor/silicon on insulator (CMOS/SOI) technology with special dopants is not currently available; however, its development may enable commercial cellular telephone technology to be exploited for the production of inexpensive mass-produced thermal neutron detectors. One could envision combining such technology with tracking technology based on GPS so that one could monitor the neutron state of a given container as it moved around the world. This type of technology might have further application as a general detector for use throughout the U.S. infrastructure. While the technology appears promising, there is no database on its actual utility in real world applications.

There are also active techniques for penetrating a shipping container in an effort to find nuclear materials. One example of this is the pulsed neutron source. A high-energy neutron produced, for example, from the D–T reaction is fired into the shipping container to interact through inelastic scattering with the elements in the material under investigation. Gamma radiation would be searched for to see if the radiation characteristic of a particular material is detected. These devices are relatively large and would be suitable only in a port environment. The devices and the interpretation of the signatures measured require a high degree of sophistication. It should be noted that this approach has application to detection of materials other than nuclear materials, for example, for nitrogen in conventional explosives.

Another active detection device is the gamma ray scanner, a large device intended to image the inside of the shipping container. It is quite well understood and might form the backbone of any port container inspection system.

**there are also active techniques for penetrating a shipping container in an effort to find nuclear materials**

## Explosive Detection

Explosive detection systems generally fall into two categories: bulk detection and vapor phase detection. Several of the techniques typically utilized in each of these detection categories are listed in table 2. The gamma ray imagers and pulsed neutron detectors were mentioned in the discussion of nuclear materials detection. Both nuclear magnetic resonance and nuclear quadrupole resonance are techniques that will not detect explosives through metallic containers and are therefore not suitable for the rapid screening of shipping containers. Use of a vapor phase detector, which works off the natural vapor pressure associated with explosives, would most likely involve extracting an air sample from a closed shipping container and examining the sample. The vapor pressure of explosives varies over quite a wide range. For example, when compared with the concentration of molecules in air, the vapor pressures of EGDN, DNT, and NG fall in the range of parts per million. However, the vapor pressures for ammonium nitrate and TNT fall in the range of parts per billion. The modern explosives RDX, PETN, and HMX have vapor pressures in the range of parts per trillion. Table 3 provides the practical detection capabilities of the various vapor detectors listed in table 2. Since the vapor pressure represents the maximum vapor concentrations that could exist in the closed container, it is clear from table 3 that detection of explosives through the vapor pressure technique will be difficult in the near term. However, there have been promising developments.[11]

## Chemical and Biological Detection

Technologies used for the detection of chemical agents in a container will probably be similar to those for the detection of

**Table 2. Examples of Explosive Detectors**

| Bulk Detectors | Vapor Detectors |
|---|---|
| Gamma ray and X-ray | Ion mobility spectrometry |
| Neutron (thermal, fast, pulsed fast) | Gas chromatography |
| Nuclear magnetic resonance (NMR) | Chemiresistor |
| Nuclear quadrupole resonance (NQR) | Fluorescent polymer |

**Table 3. Comparison of Vapor Pressure Detection**

| System | Detection Limits | Limitations |
|---|---|---|
| Ion mobility spectrometer | Parts/billion | Must be close to explosive or chemical, noise limits become problems at low signal levels, fundamental problems in selectivity and resolution, shows promise for increased detectioin in low concentration |
| Chemical resistors | Parts/billion | Must be close to explosive or chemical, needs improved signal-to-noise ratio (SNR) |
| Fluorescent polymers | Parts/trillion (in principle) | Must be close to explosive or chemical, needs improved SNR, demonstrated at parts/billion in reliable system |
| Gas chromatography + sound acoustic wave | Parts/billion | Must be close to explosive or chemical, must be able to desorb the explosive vapors for system to be useful |

explosives. Chemical agents, such as nerve agents, typically have rather high vapor pressures ranging from a few thousandths of an atmosphere for Sarin to a millionth of an atmosphere for VX. If a container holding a nerve agent is leaking, the vapor phase detectors discussed previously very likely would provide a detection. The design of weaponized chemical agent containers, however, precludes leaking. Therefore, it is unlikely that militarized chemical agents would be detected using these technologies.

The detection of biological agents shipped in seaborne containers presents the most difficult problem. Since biological agents have no vapor pressure and in all likelihood would be shipped in small quantity and therefore be well hidden, current detector technology probably would be ineffective.

The immediate deployment of gamma ray imaging technology and other current detectors to address the threat from radiological weapons is recommended. A gamma ray imager might also be developed along with other existing technologies to create a single point, multipurpose detector. The imager would provide a degree of visual inspection capability to examine the contents of the shipping container that could be supplemented with one or more of the nuclear detection technologies mentioned above. If an air sample could be drawn from the container, it would be possible to test for chemical agents and explosive vapors. However, for the reasons stated above, detection seems unlikely.

One of the most important questions regarding detectors is how best to employ a particular technology. The study recognized the importance of introducing technological screening devices that could be incorporated into the container transportation process in a nonintrusive manner at both the ports of origin and destination. To minimize costly delays, the detector must be capable of sampling individual containers without unduly interrupting their movement between the ship and various land transport systems. Detectors currently in use or proposed for development might be employed in four ways: detectors incorporated into devices used to handle the container box; fixed, pass-through detectors that scan containers as they move through or near the device; mobile detectors ranging from hand-held to truck-mounted devices; and detectors incorporated into the container box. For example, proposals exist to incorporate detection systems into the cranes that lift containers between the ship and pier or to pass containers through scanning devices by truck or rail. Further research will be needed to determine which detector or combination of detectors will prove most cost effective.

**an effective virtual border strategy will require a great deal of coordination and cooperation among the responsible parties involved, both domestically and internationally**

For the long term, it is quite clear that a substantial program is needed to move promising detection technology from the laboratory to the port. An important first step toward establishing a port detector program is to create a technology investment plan that would identify promising areas of research and help prioritize investments. A technology investment plan might also be used to coordinate science and technology resources among government agencies developing detectors and to optimize investment expenditures by eliminating duplication of effort among these agencies.

## Creating the Virtual Border

Assembling the pieces of an effective virtual border strategy will require a great deal of coordination and cooperation among the responsible parties involved, both domestically and internationally. If the virtual border concept is to work, a unified, international program must take into account not just the cross-cutting lines of responsibility and authority of the U.S. interagency process but also the economic realities of the commercial trade industry and the interests of our international trading partners. Part of the challenge in constructing a virtual border program is the issue of cost versus risk. Where do we find the funding for this program? How many dollars should be spent, and what is the fair proportion of these expenditures between the U.S. Government and our overseas partners? How do we measure the effectiveness of the program?

Currently, no single U.S. Government agency has final accountability for seaborne container security. In fact, the Customs Service, Coast Guard, agencies within the Departments of Transportation, Commerce, and Agriculture, the Immigration and Naturalization Service, Maritime Administration, and numerous state and local entities all have jurisdiction over various parts of container commerce, shipping, and port operations. Recognizing the difficulty of coordinating across departments, President George W. Bush proposed in June 2002 the creation of a single department whose primary mission is to protect the homeland. The Department of Homeland Security would be charged with, among other responsibilities, preventing terrorists and explosives from entering the country and bringing together scientists to develop technologies that detect biological, chemical, and nuclear weapons.[12] Under this proposal, the U.S. Customs Service, Coast Guard, and Transportation Security Administration would be reorganized under the new department to increase cooperation and coordination. This new department would provide the type of coordination needed to enhance container security.

As the U.S. Government moves forward with the implementation of a container security program, it must do so in concert with the business community. Government and commercial cooperation is necessary to ensure that proposed security measures are readily incorporated into existing commercial practices or introduced in such a way as to minimize the disruption to commerce. Wherever possible, the goal should be to achieve voluntary compliance with new security requirements for container shipping and port operations.

The virtual border approach requires a high degree of international cooperation. Exporting states need to assume greater responsibility for the security of container shipping originating from or passing through their ports. In the near term, increased cooperation between the United States and foreign governments will improve coordination in the collection and sharing of container cargo shipping information and will heighten physical security at ports and facilities through which container traffic moves. The United States will also need to work with its trading partners to facilitate the creation of trusted shipping agents and, where warranted, to create a more prominent role for U.S. Customs at foreign ports that might include more on-site inspectors and detection equipment. Such measures will likely require reciprocal improvements at U.S. port facilities, including stricter inspection of exported containers and potentially allowing foreign inspectors in U.S. ports. In fact, it is realistic to assume that our trading partners will expect us to introduce the same measures domestically as those we advocate overseas. In addition to foreign governments, cooperation with international organizations, such as the International Maritime Organization (IMO) and the World Customs Organization, will be needed. Some efforts in both organizations are currently under way. Recognizing container terrorism as a potential international problem, the IMO, for example, recommended enhanced physical security at port facilities and improved inspection processes. As security measures are introduced, U.S. security as well as the security of global trade will likely improve.

**exporting states need to assume greater responsibility for the security of container shipping originating from or passing through their ports**

Rather than designing a comprehensive container security program for future implementation, the process should be started immediately through an incremental approach similar to spiral development currently used by the Department of Defense for major systems development. In spiral development, pieces of the system are built and tested, and improvements are made based on a continuous series of operational performance evaluations. The nature of container threats is well enough understood that a similar demonstration program could be constructed for a virtual border prototype. The initial phase would include identifying shipping elements needed to establish threat profiles, specifying a standard electronic reporting format, and establishing links between various databases, such as those shown in figure 2. Representing an existing baseline capability, the National Maritime Intelligence Center in Suitland, Maryland, could serve as the data fusion center recommended by this study. During its transition, agreements could be negotiated with Singapore, Hong Kong, Rotterdam, or one of the other mega-ports to serve as a prototype development test site. This spiral development process would also include a continuous red team evaluation of the most probable threat scenarios. Red teams will prove to be a critical element in identifying necessary changes to the baseline system, especially as advanced computational techniques are introduced into the container profiling process.

## Moving Ahead

Since the completion of this study, a number of steps toward the implementation of a virtual border security program have been taken. An interagency container working group, sponsored by the Office of Homeland Security, was formed in December 2001. This group's recommendations closely mirror the findings of this study in a number of areas. These include the need for government and business coordination, improving container cargo data collection and analysis, improving the physical security of containers, working with our trading partners abroad, and utilizing advanced detector technologies to enhance the inspection process.

**Defense Horizons** *is published by the Center for Technology and National Security Policy through the Publication Directorate of the Institute for National Strategic Studies, National Defense University.* **Defense Horizons** *and other National Defense University publications are available online at http://www.ndu.edu/inss/press/nduphp.html.*



*Center for Technology and National Security Policy*

**Hans Binnendijk**
Director

Legislation under way introduces many of the improvements recommended by this study. The Maritime Transportation Antiterrorism Act of 2002 calls for the development and maintenance of an antiterrorism cargo identification and screening system and improvements in the physical security of containers. This legislation also provides for the electronic submission of containerized cargo information no later than 24 hours before a cargo is loaded on a vessel and the electronic reporting of crew and passenger manifests. The Port and Maritime Security Act of 2001 focuses on port vulnerabilities and ways to enhance security at port facilities. Though it does not specifically address physical security of containers, it does call for electronic submission of cargo manifest and crew information, development of nonintrusive screening and detection equipment, credentialing of port personnel, and improved collection and coordination of maritime intelligence. These provisions and other proposed improvements similar to the virtual border construct introduce changes that will significantly enhance maritime security.

Over the past few decades, international containerized shipping has evolved to become the main artery of global trade, providing both convenient and inexpensive access to goods from markets around the world. Yet the very size and efficiencies that have made container shipping such an attractive means of transport have also created a system that is highly vulnerable to terrorist exploitation. Unless fundamental changes in the practices of the current system are introduced, the possibility of seaborne container terrorism will remain a significant threat. But proposals to alter current container shipping business practices must balance security concerns with economic imperatives, lest global commerce be severely disrupted. The virtual border proposal seeks to achieve this balance. It addresses both the need to provide a comprehensive, multilayered defense against terrorism and to minimize disruptions to the functioning of an orderly international system.

The notion of extending U.S. control over container shipping beyond our traditional borders that is embodied in the virtual border concept presents a number of challenges. The timely collection and analysis of data required for cargo certification and profiling, improvements in the physical security of container shipping, and the development and introduction of sophisticated detection systems, all key elements of the virtual border concept, require an unprecedented level of domestic and international cooperation. Without such cooperation, no security program can hope to be effective. It is encouraging to note that recognition of the potential container problem is now widespread, and some progress has been achieved. Current U.S. interagency efforts, pending Federal legislation on maritime security, international discussion, and especially the proposal to create the Department of Homeland Security, are steps in the right direction. Designing a foolproof system is simply not possible, but if these current efforts lead to the establishment of a virtual border security program, the risk of a seaborne container terrorist attack will be substantially reduced.

## *Notes*

[1] The CTNSP core study team consisted of Hans Binnendijk, Leigh C. Caraher, Timothy Coffey, and H. Scott Wynfield. Desmond Saunders-Newton provided consultation concerning advanced computing. Col Steven Tomisek, USMC, represented the National Defense University (NDU) Institute for National Strategic Studies (INSS). Groups consulted include the U.S. Coast Guard, Customs, Navy, Freight Desk Technologies, Logistics Management Institute, Natural Selections, IBM, World Shipping, Booz-Allen and Hamilton, and other members of NDU and INSS.

[2] Testimony of Christopher Koch, president and CEO of The World Shipping Council, before the Senate Committee on Commerce, Science and Transportation, Charleston, SC, February 19, 2002. The World Shipping Council notes that these estimates are based on liner shipping, that is, those vessels operating on regular, scheduled services and fixed routes. Estimates exclude bulk carriers operating for hire on an as needed, where needed basis.

[3] Louis Sahagun, "Really Big Doings at the Ports," *The Los Angeles Times,* March 28, 2002.

[4] Testimony of Senator Ernest F. Hollings (D–SC), Committee on Government Affairs, Hearing on Seaport Vulnerability, December 6, 2001.

[5] As a basis for comparison, the most common size international standard container, at 40 feet in length, has several times the cargo capacity of the rental truck used in the 1995 attack on the Alfred E. Murrah Federal Building in Oklahoma City.

[6] One potential source for radiological material is the compact radio thermal generators scattered throughout the former Soviet Union (some of which are now apparently missing) that contain sufficient quantities of strontium 90 to form the basis for a dirty bomb. The subsequent capture and interrogation of Abu Zubaydah, a top bin Laden lieutenant, indicates that al Qaeda may have been trying to develop just such a weapon.

[7] Testimony of Rob Quartel, chairman and CEO, Freight Desk Technologies, before the Government Affairs Committee of the U.S. Senate, December 6, 2001.

[8] The depiction of the container domain in figure 1 is based on an original presentation by Freight Desk Technologies.

[9] John Simpson, president of the American Association of Exporters and Importers, quoted in William Booth, "Where Sea Meets Shore, Scenarios for Terrorists," *The Washington Post,* January 3, 2002.

[10] The study team's visit to a large East Coast port confirmed that only modest onsite improvements toward stopping container terrorism have been introduced. Shortages of inspectors and the lack of automated processes hamper counterterrorist efforts.

[11] This analysis does not refer to vapor phase detection techniques being applied to residues of explosives manually collected, for example, by taking swabs. This approach is simply not practical in the situation envisioned.

[12] George W. Bush, address to the Nation on the Department of Homeland Security, June 6, 2002.

# The *Defense* Horizons Series

**Number 1, June 2001**
## Managing Change: Capability, Adaptability, and Transformation
*Hans Binnendijk and Richard L. Kugler*

**Number 2, September 2001**
## Resurrecting Transformation for the Post-Industrial Era
*Douglas A. Macgregor*

**Number 3, October 2001**
## UCAV Technological, Policy, and Operational Challenges
*Charles L. Barry and Elihu Zimet*

**Number 4, October 2001**
## Maritime Access: Do Defenders Hold All the Cards?
*Arthur H. Barber III and Delwyn L. Gilmore*

**Number 5, November 2001**
## Adapting Forces to a New Era: Ten Transforming Concepts
*Hans Binnendijk and Richard L. Kugler*

**Number 6, December 2001**
## Current Export Policies: Trick or Treat?
*David R. Oliver, Jr.*

**Number 7, February 2002**
## Global Trade: America's Achilles' Heel
*James M. Loy and Robert G. Ross*

**Number 8, February 2002**
## Small Security: Nanotechnology and Future Defense
*John L. Petersen and Dennis M. Egan*

**Number 9, March 2002**
## Nonlethal Capabilities: Realizing the Opportunities
*E.R. Bedard*

**Number 10, March 2002**
## Rediscovering the Infantry in a Time of Transformation
*Bing West*

**Number 11, April 2002**
## Computer Games and the Military: Two Views
*J.C. Herz and Michael R. Macedonia*

**Number 12, April 2002**
## The Airborne Laser from Theory to Reality: An Insider's Account
*Hans Mark*

**Number 13, May 2002**
## Relevancy and Risk: The U.S. Army and Future Combat Systems
*Joseph N. Mait and Jon G. Grossman*

**Number 14, June 2002**
## Toward Missile Defenses from the Sea
*Hans Binnendijk and George Stewart*

**Number 15, July 2002**
## Biological Weapons: Toward a Threat Reduction Strategy
*Brad Roberts and Michael Moodie*